PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-204229
(43)Date of publication of application : 19.07.2002

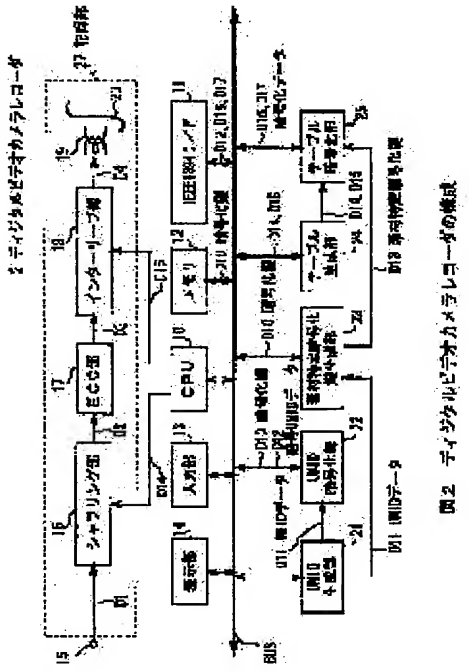
(51)Int.Cl. H04L 9/08
G06F 12/14

(21)Application number : 2000-401376
(22)Date of filing : 27.12.2000

(71)Applicant : SONY CORP
(72)Inventor : TAKAGI SATOSHI

(54) DEVICE AND METHOD FOR CIPHERING, DEVICE AND METHOD FOR DECIPHERING CIPHER, AND CIPHERING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent a ciphered object from easily being deciphered by a 3rd party.
SOLUTION: Each time respective raw materials are inputted, UMID(unique material identifier) data D11 specifying the respective raw materials are generated and the UMID data D11 corresponding to the respective raw materials are converted under mathematical conditions of a cipher key D10 to generate raw material specifying cipher keys D13 intrinsic to the respective raw materials; and mutually different data arrangement patterns (shuffling table data D14 and interleaving table data D15) corresponding to the raw materials are ciphered respectively with the raw material specifying cipher keys D13 to generate ciphered data D16 and D17 corresponding to the raw materials, thereby generating the raw material specifying cipher keys D13 which disables a 3rd party to decipher the data without knowing all of the algorithm of the cipher key D10, the conversion patterns for conversion to the raw material specifying cipher keys D13 based upon the UMID data D11 specified by the raw materials, and the UMID data D11.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－204229
（P2002－204229A）
(43)公開日　平成14年７月19日(2002.7.19)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード(参考)
Ｈ０４Ｌ　9/08		Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｈ０４Ｌ　9/00	６０１Ｃ	５Ｊ１０４
			６０１Ｅ	

審査請求　未請求　請求項の数14　ＯＬ　（全 15 頁）

(21)出願番号　特願2000－401376(P2000－401376)

(22)出願日　平成12年12月27日(2000.12.27)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　高木　聡
東京都品川区北品川６丁目７番35号ソニー株式会社内
(74)代理人　100082740
弁理士　田辺　恵基

Ｆターム(参考)　5B017 AA03 BA07
5J104 AA16 EA04 EA15 NA02

(54)【発明の名称】　暗号化装置、暗号化方法、暗号復号化装置、暗号復号化方法及び暗号化システム

(57)【要約】
【課題】第三者によって暗号化対象を容易に解読されることを防止し得るようにする。
【解決手段】各素材が入力される度にその各素材をそれぞれ特定するためのＵＭＩＤデータＤ１１を生成し、各素材にそれぞれ対応する当該ＵＭＩＤデータＤ１１を暗号化鍵Ｄ１０の数学的条件に合わせる変換を行って各素材毎に固有な素材特定暗号化鍵Ｄ１３を生成し、当該素材特定暗号化鍵Ｄ１３で各素材毎に対応したそれぞれ異なるデータ並替パターン（シャフリングテーブルデータＤ１４及びインターリーブテーブルデータＤ１５）をそれぞれ暗号化して各素材に対応した暗号化データＤ１６及びＤ１７を生成することにより、第三者にとっては暗号化鍵Ｄ１０のアルゴリズム、また素材毎に特定されたＵＭＩＤデータＤ１１に基づいて素材特定暗号化鍵Ｄ１３に変換する変換パターン、さらにはＵＭＩＤデータＤ１１の全てが分からなければ到底解読し得ない素材特定暗号化鍵Ｄ１３を生成し得る。

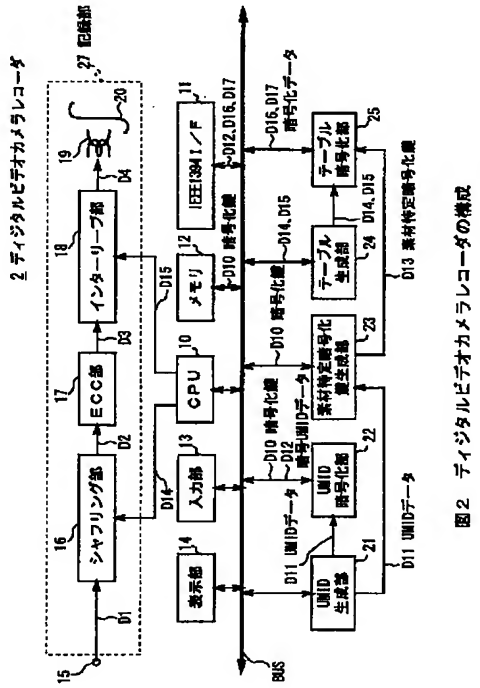


図２　ディジタルビデオカメラレコーダの構成

1

【特許請求の範囲】

【請求項１】各素材が入力される度に当該各素材をそれぞれ特定するための固有情報を生成する固有情報生成手段と、

上記各素材にそれぞれ対応する上記固有情報を所定の方式に従って変換することにより上記各素材毎に固有な暗号化鍵を生成する暗号化鍵生成手段と、

上記各素材にそれぞれ対応した上記暗号化鍵で上記各素材又は上記各素材に対応した所定の情報をそれぞれ暗号化する暗号化手段とを具えることを特徴とする暗号化装置。

【請求項２】上記各素材に対応した所定の情報は、上記各素材が入力される度に当該各素材を所定データ量単位でそれぞれ並び替えるときのデータ並替パターンであることを特徴とする請求項１に記載の暗号化装置。

【請求項３】上記固有情報生成手段は、

少なくとも上記暗号化装置を管理するための管理情報に乱数を乗じることにより上記固有情報を生成することを特徴とする請求項１に記載の暗号化装置。

【請求項４】各素材が入力される度に当該各素材をそれぞれ特定するための固有情報を生成する固有情報生成ステップと、

上記各素材にそれぞれ対応する上記固有情報を所定の方式に従って変換することにより上記各素材毎に固有な暗号化鍵を生成する暗号化鍵生成ステップと、

上記各素材にそれぞれ対応した上記暗号化鍵で上記各素材又は上記各素材に対応した所定の情報をそれぞれ暗号化する暗号化ステップとを具えることを特徴とする暗号化方法。

【請求項５】上記各素材に対応した所定の情報は、上記各素材が入力される度に当該各素材を所定データ量単位でそれぞれ並び替えるときのデータ並替パターンであることを特徴とする請求項４に記載の暗号化方法。

【請求項６】上記固有情報生成ステップは、

少なくとも上記暗号化装置を管理するための管理情報に乱数を乗じることにより上記固有情報を生成することを特徴とする請求項４に記載の暗号化方法。

【請求項７】各素材が入力される度に当該各素材をそれぞれ特定するために生成された固有情報と、当該固有情報に基づく上記各素材毎に固有な暗号化鍵で上記各素材又は上記各素材に対応した所定の情報をそれぞれ暗号化することにより生成された暗号化データとを上記暗号化装置から取得する取得手段と、

上記各素材にそれぞれ対応する上記固有情報を所定の方式に従って変換することにより上記暗号化データをそれぞれ復号化するための復号化鍵を生成する復号化鍵生成手段と、

上記各素材にそれぞれ対応する上記復号化鍵で上記暗号化データをそれぞれ復号化することにより上記各素材又は上記各素材に対応した所定の情報を復元する暗号復号化手段とを具えることを特徴とする暗号復号化装置。

2

【請求項８】各素材が入力される度に当該各素材をそれぞれ特定するために生成された固有情報と、当該固有情報に基づく上記各素材毎に固有な暗号化鍵で上記各素材又は上記各素材に対応した所定の情報をそれぞれ暗号化することにより生成された暗号化データとを上記暗号化装置から取得する取得ステップと、

上記各素材にそれぞれ対応する上記固有情報を所定の方式に従って変換することにより上記暗号化データをそれぞれ復号化するための復号化鍵を生成する復号化鍵生成ステップと、

上記各素材にそれぞれ対応する上記復号化鍵で上記暗号化データをそれぞれ復号化することにより上記各素材又は上記各素材に対応した所定の情報を復元する暗号復号化ステップとを具えることを特徴とする暗号復号化方法。

【請求項９】暗号化装置と暗号復号化装置とで構築される暗号化システムにおいて、

上記暗号化装置は、

各素材が入力される度に当該各素材をそれぞれ特定するための固有情報を生成する固有情報生成手段と、

上記各素材にそれぞれ対応する上記固有情報を所定の方式に従って変換することにより上記各素材毎に固有な暗号化鍵を生成する暗号化鍵生成手段と、

上記各素材にそれぞれ対応した上記暗号化鍵で上記各素材又は上記各素材に対応した所定の情報をそれぞれ暗号化することにより暗号化データを生成する暗号化手段と、

上記各素材にそれぞれ対応する上記固有情報と上記暗号化データとを送信する送信手段とを具え、

上記暗号復号化装置は、

上記各素材にそれぞれ対応する上記固有情報と上記暗号化データとを受信する受信手段と、

上記各素材にそれぞれ対応する上記固有情報を所定の方式に従って変換することにより上記暗号化データをそれぞれ復号化するための復号化鍵を生成する復号化鍵生成手段と、

上記各素材にそれぞれ対応する上記復号化鍵で上記暗号化データをそれぞれ復号化することにより上記各素材又は上記各素材に対応した所定の情報を復元する暗号復号化手段とを具えることを特徴とする暗号化システム。

【請求項１０】上記各素材に対応した所定の情報は、上記各素材が入力される度に当該各素材を所定データ量単位でそれぞれ並び替えるときのデータ並替パターンであることを特徴とする請求項９に記載の暗号化システム。

【請求項１１】上記固有情報生成手段は、

少なくとも上記暗号化装置を管理するための管理情報に乱数を乗じることにより上記固有情報を生成することを特徴とする請求項９に記載の暗号化システム。

【請求項１２】暗号化装置と暗号復号化装置とで構築さ

れる暗号化システムにおいて、
上記暗号化装置は、
各素材が入力される度に当該各素材をそれぞれ特定するための固有情報を生成する固有情報生成手段と、
上記各素材にそれぞれ対応する上記固有情報を所定の方式に従って変換することにより上記各素材毎に固有な暗号化鍵を生成する暗号化鍵生成手段と、
上記各素材にそれぞれ対応した上記暗号化鍵で上記各素材又は上記各素材に対応した所定の情報をそれぞれ暗号化することにより暗号化データを生成する暗号化手段と、
上記各素材にそれぞれ対応する上記固有情報と上記暗号化データとを所定の記憶媒体に記録する記憶手段とを具え、
上記暗号復号化装置は、
上記記憶媒体から上記各素材にそれぞれ対応する上記固有情報と上記暗号化データとを読み出す読み出し手段と、
上記各素材にそれぞれ対応する上記固有情報を所定の方式に従って変換することにより上記暗号化データをそれぞれ復号化するための復号化鍵を生成する復号化鍵生成手段と、
上記各素材にそれぞれ対応する上記復号化鍵で上記暗号化データをそれぞれ復号化することにより上記各素材又は上記各素材に対応した所定の情報を復元する暗号復号化手段とを具えることを特徴とする暗号化システム。
【請求項１３】上記各素材に対応した所定の情報は、上記各素材が入力される度に当該各素材を所定データ量単位でそれぞれ並び替えるときのデータ並替パターンであることを特徴とする請求項１２に記載の暗号化システム。
【請求項１４】上記固有情報生成手段は、
少なくとも上記暗号化装置を管理するための管理情報に乱数を乗じることにより上記固有情報を生成することを特徴とする請求項１２に記載の暗号化システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は暗号化装置、暗号化方法、暗号復号化装置、暗号復号化方法及び暗号化システムに関し、例えばディジタルビデオカメラレコーダとディジタルビデオテープレコーダとで構築される暗号化システムに適用して好適なものである。
【０００２】
【従来の技術】従来、ディジタルビデオテープレコーダ（以下、これをビデオテープレコーダと呼ぶ）は、撮影者の操作によりディジタルビデオカメラレコーダ（以下、これをビデオカメラと呼ぶ）でビデオカセットの磁気テープに記録された画像データを再生することにより外部モニタに再生映像を表示するようになされている。
【０００３】しかしながらビデオテープレコーダにおいては、撮影者の意図しない第三者によって再生操作された場合でも、再生映像を外部モニタに表示してしまうので、意図しない第三者に容易に当該再生映像が視認されてしまっていた。
【０００４】このような問題を解決する１つの方法としては、撮像することにより得られた画像データに対して所定の暗号アルゴリズムに基づく暗号化処理を施した後にビデオカセットの磁気テープに記録するビデオカメラと、そのビデオカセットを再生する際、当該ビデオカメラの場合と同じ暗号アルゴリズムに基づく復号化処理を施すことにより元の画像データを復元するビデオテープレコーダとで暗号化システムを構築することが考えられる。
【０００５】
【発明が解決しようとする課題】ところでかかる暗号化システムにおいては、ビデオカメラによって常時同じ暗号アルゴリズムに基づく暗号化処理を施しているので、その暗号アルゴリズムが意図しない第三者によって解読された場合には、そのビデオカメラで撮像されたビデオカセットの再生映像が全てビデオテープレコーダを介して視認されてしまうという問題がある。
【０００６】本発明は以上の点を考慮してなされたもので、第三者によって容易に暗号化対象が解読されることを防止し得る暗号化装置、暗号化方法、暗号復号化装置、暗号復号化方法及び暗号化システムを提案しようとするものである。
【０００７】
【課題を解決するための手段】かかる課題を解決するため本発明においては、各素材が入力される度に当該各素材をそれぞれ特定するための固有情報を生成し、各素材にそれぞれ対応する固有情報を所定の方式に従って変換して各素材毎に固有な暗号化鍵を生成し、その暗号化鍵で各素材又は各素材に対応した所定の情報をそれぞれ暗号化することにより、類推し難い固有情報の全てが分からなければ第三者にとっては到底解読し得ない固有な素材毎の暗号化鍵を生成することができるので、当該第三者によって容易に暗号化対象が解読されることを防止し得る。
【０００８】また各素材毎に対応した所定の情報として、各素材が入力される度にその各素材を所定データ量単位でそれぞれ並び替えるためのデータ並替パターンを暗号化するようにしたことにより、素材そのものを暗号化するよりも一段と少ないデータ量で暗号化することができる。
【０００９】またかかる課題を解決するため本発明においては、各素材が入力される度に当該各素材をそれぞれ特定するために生成された固有情報と、当該固有情報に基づく各素材毎に固有な暗号化鍵で各素材又は各素材に対応した所定の情報をそれぞれ暗号化して生成された暗号化データとを暗号化装置から取得し、各素材にそれぞ

れ対応する固有情報を所定の方式に従って変換して暗号化データをそれぞれ復号化するための復号化鍵を生成し、その復号化鍵で暗号化データをそれぞれ復号化して各素材又は各素材に対応した所定の情報を復元することにより、類推し難い固有情報と、当該固有情報に基づいて生成されているために第三者にとっては到底解読し得ない固有な素材毎の暗号化鍵とを取得して復号化鍵を生成することができるので、確実かつ正確に各素材又は各素材に対応した所定の情報毎を復元し得る。

【００１０】さらにかかる課題を解決するため本発明においては、各素材が入力される度に当該各素材をそれぞれ特定するための固有情報を生成し、各素材にそれぞれ対応する固有情報を所定の方式に従って変換して各素材毎に固有な暗号化鍵を生成し、その暗号化鍵で各素材又は各素材に対応した所定の情報をそれぞれ暗号化して暗号化データを生成し、暗号化データと固有情報とを送信する暗号化装置と、当該暗号化データと固有情報とを受信し、各素材にそれぞれ対応する固有情報を所定の方式に従って変換して暗号化データをそれぞれ復号化するための復号化鍵を生成し、その復号化鍵で暗号化データをそれぞれ復号化して各素材又は各素材に対応した所定の情報を復元する暗号復号化装置とを構築することにより、暗号化装置では、類推し難い固有情報の全てが分からなければ第三者にとっては到底解読し得ない固有な素材毎の暗号化鍵を生成することができるので、当該第三者によって容易に暗号化対象が解読されることを防止し得、暗号復号化装置では、送信手段を介して類推し難い固有情報と、当該固有情報に基づいて生成されているために第三者にとっては到底解読し得ない固有な素材毎の暗号化鍵とを受信して復号化鍵を生成することができるので、確実かつ正確に各素材又は各素材に対応した所定の情報毎を復元し得る。

【００１１】さらにかかる課題を解決するため本発明においては、各素材が入力される度に当該各素材をそれぞれ特定するための固有情報を生成し、各素材にそれぞれ対応する固有情報を所定の方式に従って変換して各素材毎に固有な暗号化鍵を生成し、その暗号化鍵で各素材又は各素材に対応した所定の情報をそれぞれ暗号化して暗号化データを生成し、暗号化データと固有情報とを所定の記憶媒体に記憶する暗号化装置と、その暗号化データと固有情報とを当該記憶媒体から読み出し、各素材にそれぞれ対応する固有情報を所定の方式に従って変換して暗号化データをそれぞれ復号化するための復号化鍵を生成し、その復号化鍵で暗号化データをそれぞれ復号化して各素材又は各素材に対応した所定の情報を復元する暗号復号化装置とを構築することにより、暗号化装置では、類推し難い固有情報の全てが分からなければ第三者にとっては到底解読し得ない固有な素材毎の暗号化鍵を生成することができるので、当該第三者によって容易に暗号化対象が解読されることを防止し得、暗号復号化装

置では、記憶手段から読み出した類推し難い固有情報と、当該固有情報に基づいて生成されているために第三者にとっては到底解読し得ない固有な素材毎の暗号化鍵とを受信して復号化鍵を生成することができるので、確実かつ正確に各素材又は各素材に対応した所定の情報毎を復元し得る。

【００１２】

【発明の実施の形態】以下図面について、本発明の一実施の形態を詳述する。

【００１３】（１）ネットワーク対応型暗号化システム

図１において、１は全体として本発明によるネットワーク対応型暗号化システムを示し、ディジタルビデオカメラレコーダ（以下、これをビデオカメラと呼ぶ）２と、ディジタルビデオテープレコーダ（以下、これをビデオテープレコーダと呼ぶ）３とが互いにパーソナルコンピュータ（図示せず）を介してそれぞれインターネット４に接続されており、ディジタルビデオカメラ２とビデオテープレコーダ３との間で各種情報の授受を行い得るようになされている。

【００１４】このネットワーク対応型暗号化システム１では、ビデオカメラ２において撮像して得られた素材である画像データに所定の処理を施して記録したビデオカセット５がビデオテープレコーダ３に装填されて再生されるようになされている。

【００１５】（２）ビデオカメラにおける暗号化処理手順

図２に示すような回路構成のビデオカメラ２を用いて本実施の形態における暗号化処理手順を説明する。

【００１６】このビデオカメラ２は、ＣＰＵ(Central Processing Unit）１０、他の機器（本実施の形態の場合はパーソナルコンピュータ）との間で各種情報の授受を行うＩＥＥＥ(Institute of Electrical and Electronics Engineers）１３９４インターフェイス（Ｉ／Ｆ）１１、メモリ１２、各種操作ボタン（図示せず）等の設けられた入力部１３、液晶ディスプレイでなる表示部１４及び暗号化部２６がそれぞれデータバスＢＵＳを介して互いに接続されており、当該ＣＰＵ１０がメモリ１２から読み出した各種プログラムに従って所定の処理を実行することによりビデオカメラ２を統括的に制御し、記録部２７によりビデオカセット５（図１）の磁気テープ２０に対して記録処理を実行するようになされている。

【００１７】実際上、図３において、ＣＰＵ１０は、ルーチンＲＴ１に従った暗号化処理手順の開始ステップからステップＳＰ１に移る。

【００１８】ステップＳＰ１においてＣＰＵ１０は、まず最初にビデオテープレコーダ３からインターネット４（図１）を経由して送信された非対象暗号化方式であるＲＳＡに従った暗号化鍵Ｄ１０をＩＥＥＥ１３９４インターフェイス１１を介して予め取得してメモリ１２に記憶し、次のステップＳＰ２に移る。

【００１９】ステップＳＰ２においてＣＰＵ１０は、入力部１３の記録ボタンが撮影者によって押下されたか否かを判断する。ここで否定結果が得られると、ＣＰＵ１０は記録ボタンが押下されるまで待ち受ける。これに対して肯定結果が得られると、ＣＰＵ１０は次のステップＳＰ３に移る。

【００２０】ステップＳＰ３においてＣＰＵ１０は、ＵＭＩＤ生成部２１によって、メモリ１２に記憶されている各種情報やシステムクロック等に基づいて画像データや音声データ等の素材を特定するためのＵＭＩＤ(Unique Material IDentifier)を生成し、当該ＵＭＩＤのうち一部分をＵＭＩＤデータＤ１１として抽出し、これをＵＭＩＤ暗号化部２２及び素材特定暗号化鍵生成部２３に送出し、次のステップＳＰ４に移る。

【００２１】ここで、ＵＭＩＤのデータ構造について説明する。図４において、ＵＭＩＤは、基本ＵＭＩＤと延長ＵＭＩＤとの 64 [byte]から構成され、基本ＵＭＩＤは当該ＵＭＩＤであること等を表す 12 [byte]のユニバーサルラベル、データの長さを表す 1 [byte] のデータ長、ダビング回数を表す 3 [byte] のインストナンバ及びビデオカメラ２もしくはそのビデオカメラ２内のチップ固有のシリアルナンバに乱数を乗じることにより固有な情報として生成された 16 [byte]のマテリアルナンバを含む全 32 [byte]で構成される。

【００２２】また延長ＵＭＩＤは、ビデオカメラ２内のシステムクロックに基づく日及び時刻を表す 8 [byte] の日時、ＧＰＳ(Global Positioning System) 機能を有するビデオカメラの場合には、そのビデオカメラの存在位置を表す 12 [byte]の位置情報、国を表す 4 [byte] の国コード、組織を表す 4 [byte] の組織コード及びユーザを表す 4 [byte] のユーザ名を含む全 32 [byte]で構成される。

【００２３】この実施の形態の場合、ＣＰＵ１０は、かかるＵＭＩＤのうち固有な情報であるマテリアルナンバを含む基本ＵＭＩＤをＵＭＩＤデータＤ１１として抽出するようになされており、当該マテリアルナンバによって素材を特定し得るようになされている。

【００２４】このようにＣＰＵ１０は、撮影者によって記録ボタンが押下される毎に素材を特定するための新たなＵＭＩＤデータＤ１１を生成するようになされている。

【００２５】ステップＳＰ４においてＣＰＵ１０は、メモリ１２に記憶しておいた暗号化鍵Ｄ１０をＵＭＩＤ暗号化部２２及び素材特定暗号化鍵生成部２３に送出し、次のステップＳＰ５に移る。

【００２６】ステップＳＰ５においてＣＰＵ１０は、素材特定暗号化鍵生成部２３によって、素材を特定するためのＵＭＩＤデータＤ１１を暗号化鍵Ｄ１０に基づく数学的条件に合わせて変換することにより、素材固有の暗号化鍵である素材特定暗号化鍵Ｄ１３を生成する。

【００２７】またＣＰＵ１０は、ＵＭＩＤ暗号化部２２によって、ビデオテープレコーダ３において素材特定暗号化鍵Ｄ１３を復号化するために必要なＵＭＩＤデータＤ１１に対して、ビデオテープレコーダ３から送信された暗号化鍵Ｄ１０で暗号化処理を施して暗号ＵＭＩＤデータＤ１２を生成することにより、インターネット４を経由してビデオテープレコーダ３に送信する際、第三者によって解読されることを防止し得るようになされている。

【００２８】そしてＣＰＵ１０は、素材特定暗号化鍵Ｄ１３をテーブル暗号化部２５に送出すると共に、暗号ＵＭＩＤデータＤ１２を一旦メモリ１２に記憶した後、次のステップＳＰ６に移る。

【００２９】ステップＳＰ６においてＣＰＵ１０は、例えば図５に示すようなパターン決定画面１４Ａを表示部１４に表示し、シャフリング部１６及びインターリーブ部１８においてデータ列の並び替えを行う際のデータ並替パターンの決定を撮影者に対して促す。

【００３０】そしてＣＰＵ１０は、パターン決定画面１４Ａを介して第１のパターン（シャフリング）項目１４Ｂ及び第２のパターン（インターリーブ）項目１４Ｃからそれぞれ所望のパターン番号が撮影者によって入力部１３から選択操作されると、当該選択された各パターン番号に対応したデータ並替パターンであるシャフリングテーブルデータＤ１４及びインターリーブテーブルデータＤ１５をテーブル生成部２４により例えば 16 Modulo 4 の関数に従って任意に生成し、次のステップＳＰ７に移る。

【００３１】因みに、ＣＰＵ１０は、記録ボタンが押下される毎に新たに生成するＵＭＩＤデータＤ１１と同様、記録ボタンが押下される毎にデータ並替パターンを撮影者に選択させることにより、素材毎に新たなシャフリングテーブルデータＤ１４及びインターリーブテーブルデータＤ１５を生成するようになされている。

【００３２】ステップＳＰ７においてＣＰＵ１０は、シャフリングテーブルデータＤ１４をシャフリング部１６に送出し、インターリーブテーブルデータＤ１５をインターリーブ部１８に送出することにより、シャフリング部１６及びインターリーブ部１８に対してそれぞれデータ並替パターンを設定すると共に、当該シャフリングテーブルデータＤ１４及びインターリーブテーブルデータＤ１５をテーブル生成部２４からテーブル暗号化部２５に送出し、次のステップＳＰ８に移る。

【００３３】ステップＳＰ８においてＣＰＵ１０は、テーブル暗号化部２５によって、シャフリング部１６及びインターリーブ部１８でそれぞれ設定したシャフリングテーブルデータＤ１４及びインターリーブテーブルデータＤ１５に対して、素材特定暗号化鍵生成部２３から供給された素材固有の暗号化鍵である素材特定暗号化鍵Ｄ１３で暗号化処理を施すことにより、インターネット４

（図１）を経由してビデオテープレコーダ３へ送信する際に第三者に解読されることがないように暗号化データＤ１６及びＤ１７を生成し、これらを一旦メモリ１２に記憶した後、次のステップＳＰ９に移る。

【００３４】ステップＳＰ９においてＣＰＵ１０は、上述のステップＳＰ２で記録ボタンが押下されたことにより撮像して得られた素材である画像データに対してＭＰＥＧ２(Moving Picture Experts Group-layer 2)方式の圧縮符号化処理が施されたエレメンタルストリームＤ１を入力端１５を介して記録部２７のシャフリング部１６に入力する。

【００３５】シャフリング部１６は、上述のステップＳＰ７で設定されたシャフリングテーブルデータＤ１４のデータ並替パターンに従って、エレメンタルストリームＤ１の１フレーム分の各マクロブロックを並び替えるシャフリングを施す。

【００３６】このシャフリングの主たる目的としては、磁気テープ上へのマクロブロックの記録位置を分散させることにより、記録時とは異なるテープ速度で再生する変速再生時において、訂正し得なかったエラーが生じたときに再生映像を極力見易くすることにある。

【００３７】因みに、マクロブロックとは、ＭＰＥＧ２のデータ構造のうち、１６ライン×１６画素のＹ（輝度）信号ブロック４個と、当該Ｙ信号ブロック４個に対応する１６ライン×１６画素のC_r（Ｒ（赤）成分とＹ成分との色差成分）信号及びC_b（Ｂ（青）成分とＹ成分との色差成分）信号各１ブロックから構成される単位をいう。このマクロブロックは、可変長符号化されていることにより、各々のデータの長さが不揃いである。

【００３８】実際上シャフリング部１６で行われるシャフリング処理を図６及び図７において概略的に説明する。但し説明上の簡素化のため、以下、１フレームに９マクロブロックだけが含まれているものと仮定する。

【００３９】図６において、シャフリング部１６は、走査順に並ぶ各マクロブロックＭＢ１～ＭＢ９を、テーブル生成部２４から供給されたシャフリングテーブルデータＤ１４に従って、予め指定された内部メモリのメモリマップへランダムに書き込むことによりシャフリングを施す。

【００４０】このときシャフリング部１６は、図７に示すように、可変長データである各マクロブロックを、磁気テープ２０上に記録する際の単位である固定長枠（以下、これをシンクブロックと呼ぶ）に分割し、当該シンクブロックよりも長い各オーバーフロー部ＭＢ５′、ＭＢ２′及びＭＢ３′を一旦バッファリングし、シンクブロックに満たない（空きのある領域）マクロブロックＭＢ８、ＭＢ１、ＭＢ７及びＭＢ６の後ろに各オーバーフロー部ＭＢ５′、ＭＢ２′及びＭＢ３′を順に詰め込むことにより固定長である各シンクブロックＳＫ１～ＳＫ９を生成する。

【００４１】そしてシャフリング部１６は、各シンクブロックＳＫ１～ＳＫ９を上位又は下位番地から順に読み出し、これをＶＬＣ(Variable Length Code)データＤ２としてＥＣＣ(Error Correctig Code)部１７（図２）に送出する。

【００４２】ＥＣＣ部１７は、図８に示すように、シャフリング部１６から供給されたＶＬＣデータＤ２のシンクブロックＳＫ１～ＳＫ９を２次元的に配列し、まず垂直方向に演算してリードソロモン符号（以下、これを外符号データと呼ぶ）ＰＢ１～ＰＢ３を生成し、次に水平方向に演算してリードソロモン符号（以下、これを内符号データと呼ぶ）ＰＢ４～ＰＢ７を生成する。

【００４３】そしてＥＣＣ部１７は、外符号データＰＢ１～ＰＢ３及び内符号データＰＢ４～ＰＢ７をＶＬＣデータＤ２に付加することにより誤り訂正符号付加データＤ３を生成し、これをインターリーブ部１８（図２）に送出する。

【００４４】インターリーブ部１８は、上述のステップＳＰ７で設定されたインターリーブテーブルデータＤ１５のデータ並替パターンに従って、ＥＣＣ部１７から供給された誤り訂正符号付加データＤ３の各シンクブロックＳＫ１～ＳＫ９、外符号データＰＢ１～ＰＢ３及び内符号データＰＢ４～ＰＢ７を予め指定された内部メモリのメモリマップへランダムに書き込むことによりインターリーブを施す。

【００４５】このインターリーブの主たる目的としては、バースト誤りの影響を分散させ、誤り訂正能力を極力ランダム誤りの訂正能力に近づけることや、訂正不可能となった誤りに対して精度良好な誤り修整（コンシールメント）を行い得るようにすることである。

【００４６】因みに、バースト誤りはビット毎に独立することなく、集中的に発生する誤りのことであり、ランダム誤りは各ビット毎に不規則に生ずる誤りのことである。さらに誤り修整（コンシールメント）は、訂正不可能となった誤りによる画面上での視覚的劣化部分近傍の誤りのない画素を用いて、補間処理を施すことである。

【００４７】インターリーブ部１８は、インターリーブを施した状態において、ランダムに書き込んだ各シンクブロックＳＫ１～ＳＫ９、外符号データＰＢ１～ＰＢ３及び内符号データＰＢ４～ＰＢ７を上位又は下位番地から順に読み出し、これを記録画像データＤ４として磁気ヘッド１９を介して磁気テープ２０に記録する。

【００４８】このようにしてＣＰＵ１０は、ステップＳＰ９における記録処理を実行し、次のステップＳＰ１０に移る。

【００４９】ステップＳＰ１０においてＣＰＵ１０は、入力部１３の停止ボタンが押下されたか否かを判断する。ここで否定結果が得られると、ＣＰＵ１０はステップＳＰ９に戻って記録処理を続ける。

【００５０】これに対して肯定結果が得られると、ＣＰ

Ｕ１０は記録処理を停止し、次のステップＳＰ１１に移る。

【００５１】この場合、磁気テープ２０に記録された記録画像データＤ４をビデオテープレコーダ３が再生するには、記録画像データＤ４を生成する過程で行ったデータ並替パターン（シャフリングテーブルデータＤ１４及びインターリーブテーブルデータＤ１５）を認識し、当該データ並替パターンとは逆のデータ並戻パターンを用いてデータの並び戻しを行う必要がある。

【００５２】従ってＣＰＵ１０は、上述のステップＳＰ５でメモリ１２に一旦記憶した暗号ＵＭＩＤデータＤ１２と、上述のステップＳＰ８でメモリ１２に一旦記憶した暗号化データＤ１６及びＤ１７とをビデオテープレコーダ３に送信しなければならない。

【００５３】ステップＳＰ１１においてＣＰＵ１０は、メモリ１２に一旦記憶していた暗号ＵＭＩＤデータＤ１２、暗号化データＤ１６及びＤ１７をメモリ１２から読み出し、これらをＩＥＥＥ１３９４インターフェイス１１からパーソナルコンピュータ（図示せず）及びインターネット４（図１）を順次介してビデオテープレコーダ３に送信した後、再度ステップＳＰ２に移って、上述の処理を繰り返す。

【００５４】このように、ビデオカメラ２は、上述のルーチンＲＴ１の暗号化処理手順を入力部１３の記録ボタンが押下される度に繰り返すことにより、図９に示すように、当該記録ボタンが押下される度に入力された素材毎にそれぞれ異なるデータ並替パターンでデータ列の並び替えを行って生成した記録画像データＤ４（Ｄ４Ａ～Ｄ４Ｎ）を順次磁気テープ２０に記録するようになされている。

【００５５】さらにＣＰＵ１０は、記録ボタンが押下される度に入力された素材毎にそれぞれを特定するためのＵＭＩＤデータＤ１１を暗号化鍵Ｄ１０で暗号化することにより暗号ＵＭＩＤデータＤ１２（Ｄ１２Ａ～Ｄ１２Ｎ）を生成すると共に、そのＵＭＩＤデータＤ１１を暗号化鍵Ｄ１０の数学的条件に合わせる変換を行うことにより素材毎に固有な素材特定暗号化鍵Ｄ１３を生成し、当該素材特定暗号化鍵Ｄ１３でそれぞれ対応するデータ並替パターンを暗号化することにより暗号化データＤ１６（Ｄ１６Ａ～Ｄ１６Ｎ）、Ｄ１７（Ｄ１７Ａ～Ｄ１７Ｎ）を生成し得るようになされている。

【００５６】このようにしてＣＰＵ１０は、磁気テープ２０に記録した記録画像データＤ４（Ｄ４Ａ～Ｄ４Ｎ）をビデオテープレコーダ３で再生するために必要な暗号ＵＭＩＤデータＤ１２（Ｄ１２Ａ～Ｄ１２Ｎ）及び暗号化データＤ１６（Ｄ１６Ａ～Ｄ１６Ｎ）、Ｄ１７（Ｄ１７Ａ～Ｄ１７Ｎ）を当該記録画像データＤ４（Ｄ４Ａ～Ｄ４Ｎ）に対応させて生成し、これらを一旦メモリ１２に記憶しておき、記録処理が全て終了した後にパーソナルコンピュータ及びインターネット４（図１）を介してビデオテープレコーダ３に送信するようになされている。

【００５７】かくしてＣＰＵ１０は、記録画像データＤ４（Ｄ４Ａ～Ｄ４Ｎ）に対応したデータ並替パターン（シャフリングテーブルデータＤ１４及びインターリーブテーブルデータＤ１５）を暗号化していることにより、その暗号化前のデータ並替パターンをビデオテープレコーダ３が認識できない限り元の素材に戻すことができず再生できないので、結果として素材毎に暗号化することができる。

【００５８】（３）ビデオテープレコーダにおける復号化処理手順

図１０に示すような回路構成のビデオテープレコーダ３を用いて本実施の形態における復号化処理手順を説明する。

【００５９】このビデオテープレコーダ３は、ＣＰＵ３０、他の機器（本実施の形態の場合はパーソナルコンピュータ）との間で各種情報の授受を行うＩＥＥＥ１３９４インターフェイス３１、メモリ３２、ＨＤＤ（ハードディスクドライブ）３３、各種操作ボタン（図示せず）等の設けられた入力部３４、及びビデオカメラ２に送信するための暗号化鍵Ｄ１０やその暗号化鍵Ｄ１０に対応する復号化鍵Ｄ２０を生成する鍵生成部４０がそれぞれデータバスＢＵＳを介して互いに接続されており、当該ＣＰＵ３０がＨＤＤ３３から読み出した各種プログラムに従って所定の処理を実行することによりビデオテープレコーダ３を統括的に制御し、装填されたビデオカセット５を再生部４５を介して再生するようになされている。

【００６０】因みに鍵生成部４０は、ビデオカメラ２に送信した暗号化鍵Ｄ１０に対応する復号化鍵Ｄ２０を生成し、これを予めＨＤＤ３３に記録しておくようになされている。

【００６１】実際上、ＣＰＵ３０は、ルーチンＲＴ２に従った復号化処理手順の開始ステップから次のステップＳＰ１２に移る。

【００６２】ステップＳＰ１２においてＣＰＵ３０は、ビデオカメラ２からインターネット４を経由して送信された暗号ＵＭＩＤデータＤ１２Ａ～Ｄ１２Ｎ、暗号化データＤ１６Ａ～Ｄ１６Ｎ及びＤ１７Ａ～Ｄ１７ＮをＩＥＥＥ１３９４インターフェイス３１を介して取得してＨＤＤ３３に記憶し、次のステップＳＰ１３に移る。

【００６３】ステップＳＰ１３においてＣＰＵ３０は、入力部３４の再生ボタンが押下されたか否かを判断する。ここで否定結果が得られると、ＣＰＵ３０は再生ボタンが押下されるまで待ち受ける。これに対して肯定結果が得られると、ＣＰＵ３０は次のステップＳＰ１４に移る。

【００６４】ステップＳＰ１４においてＣＰＵ３０は、ＨＤＤ３３に予め記憶しておいた復号化鍵Ｄ２０をＵＭ

ＩＤ復号化部４１及び素材特定復号化鍵生成部４２に送出する。

【００６５】そしてＣＰＵ３０は、ＨＤＤ３３に記憶した暗号ＵＭＩＤデータＤ１２Ａ～Ｄ１２Ｎのうち最初に再生する素材である記録画像データＤ４Ａに対応する暗号ＵＭＩＤデータＤ１２ＡをＵＭＩＤ復号化部４１に送出すると共に、暗号化データＤ１６Ａ及びＤ１７Ａを素材特定復号化鍵生成部４２に送出し、次のステップＳＰ１５に移る。

【００６６】ステップＳＰ１５においてＣＰＵ３０は、ＵＭＩＤ復号化部４１により暗号ＵＭＩＤデータＤ１２Ａに対してＨＤＤ３３から供給された復号化鍵Ｄ２０で復号化処理を施すことにより、元のＵＭＩＤデータＤ１１を復元し、これを素材特定復号化鍵生成部４２に送出し、次のステップＳＰ１６に移る。

【００６７】ステップＳＰ１６においてＣＰＵ３０は、素材特定復号化鍵生成部４２によりＵＭＩＤデータＤ１１を復号化鍵Ｄ２０に基づく数学的条件に合わせて変換することにより、ビデオカメラ２において生成された素材特定暗号化鍵Ｄ１３に対応する素材特定復号化鍵Ｄ２１を生成し、これをテーブル復号化部４３に送出し、次のステップＳＰ１７に移る。

【００６８】ステップＳＰ１７においてＣＰＵ３０は、テーブル復号化部４３により暗号化データＤ１６Ａ及びＤ１７Ａを素材特定復号化鍵生成部４２から供給された素材特定復号化鍵Ｄ２１でそれぞれ復号化処理を施すことにより、元のデータ並替パターンであるシャフリングテーブルデータＤ１４及びインターリーブテーブルデータＤ１５を復元し、次のステップＳＰ１８に移る。

【００６９】ステップＳＰ１８においてＣＰＵ３０は、シャフリングテーブルデータＤ１４及びインターリーブテーブルデータＤ１５にそれぞれ対応したデータ並戻パターンであるデシャフリングテーブルデータＤ２２及びデインターリーブテーブルデータＤ２３をＨＤＤ３３から読み出す。

【００７０】そしてＣＰＵ３０は、デシャフリングテーブルデータＤ２２をデシャフリング部３６に送出すると共に、デインターリーブテーブルデータＤ２３をデインターリーブ部３８に送出することにより、デシャフリング部３６及びデインターリーブ部３８に対してそれぞれデータ並戻パターンを設定し、ステップＳＰ１９に移る。

【００７１】ステップＳＰ１９においてＣＰＵ３０は、再生ボタンの押下によりビデオカセット５（図１）の磁気テープ２０から磁気ヘッド３９を介して再生された最初の記録画像データＤ４Ａをデインターリーブ部３８に入力する。

【００７２】デインターリーブ部３８は、記録画像データＤ４Ａを上述のステップＳＰ１８で設定されたデインターリーブテーブルデータＤ２３に従って、インターリーブとは逆パターンとなるデインターリーブを施すことにより元の誤り訂正符号付加データＤ３を復元し、これをＥＣＣ部３７に送出する。

【００７３】ＥＣＣ部３７は、デインターリーブ部３８から供給された誤り訂正符号付加データＤ３の内符号データＰＢ４～ＰＢ７（図８）による誤り訂正処理を施した後、外符号データＰＢ１～ＰＢ３（図８）による誤り訂正処理をも施すことにより、元のＶＬＣデータＤ２を復元し、これをデシャフリング部３６に送出する。

【００７４】デシャフリング部３６は、ＥＣＣ部３７から供給されたＶＬＣデータＤ２を上述のステップＳＰ１８で設定されたデシャフリングテーブルデータＤ２２に従って、シャフリングとは逆パターンとなるデシャフリングを施すことにより元のエレメンタルストリームＤ１を復元し、これを外部モニタに出力する。

【００７５】因みに再生部４５は、データ並替パターンを認識し得ない場合には、記録画像データＤ４を元のエレメンタルストリームＤ１に復元できず、その結果、外部モニタは画質の劣化どころか、再生者が認識し得ない映像を表示してしまうことになる。

【００７６】このようにしてＣＰＵ３０は、ステップＳＰ１９において最初の素材に対応する記録画像データＤ４Ａに対する再生処理を実行し、次のステップＳＰ２０に移る。

【００７７】ステップＳＰ２０においてＣＰＵ３０は、ビデオカセット５の磁気テープ２０から再生する記録画像データＤ４Ａが次の新たな素材に対応する記録画像データＤ４Ｂになったか否かを判断する。

【００７８】ここで肯定結果が得られると、このことは１本のビデオカセット５（図１）の磁気テープ２０に記録された複数の記録画像データＤ４のうち最初の記録画像データＤ４Ａの再生が終了したことを表しており、このときＣＰＵ３０は再度ステップＳＰ１４に戻って、次の新たな記録画像データＤ４Ｂに対応する暗号ＵＭＩＤデータＤ１２Ｂ、暗号化データＤ１６Ｂ及びＤ１７ＢをＵＭＩＤ復号化部４１及び素材特定復号化鍵生成部４２に送出し、上述の処理を繰り返し、新たな素材に対応する記録画像データＤ４Ｂに対する再生処理を実行する。

【００７９】このようにしてＣＰＵ３０は、各素材に対応する記録画像データＤ４（Ｄ４Ａ～Ｄ４Ｎ）が順次再生し終わる度に、次の素材に対応する暗号ＵＭＩＤデータＤ１２（Ｄ１２Ａ～Ｄ１２Ｎ）及び暗号化データＤ１６（Ｄ１６Ａ～Ｄ１６Ｎ）、暗号化データＤ１７（Ｄ１７Ａ～Ｄ１７Ｎ）をＵＭＩＤ復号化部４１及び素材特定復号化鍵生成部４２に送出し、上述の処理を繰り返し、記録画像データＤ４（Ｄ４Ａ～Ｄ４Ｎ）に対する再生処理を実行するようになされている。

【００８０】これに対して否定結果が得られると、このことは磁気テープ２０に記録された最初の素材に対応する記録画像データＤ４Ａの再生が終了していないことを

表しており、このときＣＰＵ３０は次のステップＳＰ２１に移る。

【００８１】ステップＳＰ２１においてＣＰＵ３０は、ビデオカセット５（図１）の磁気テープ２０を最後まで再生したか否かを判断する。ここで否定結果が得られると、このことは記録画像データＤ４Ａ～Ｄ４Ｎ全ての再生が未だ終了しておらず、再生途中であることを表しており、このときＣＰＵ３０は、再度ステップＳＰ１９に戻って再生処理を続ける。

【００８２】これに対して肯定結果が得られると、このことはビデオカセット５の磁気テープ２０に記録された素材である記録画像データＤ４Ａ～Ｄ４Ｎ全ての再生を終了したことを表しており、このときＣＰＵ３０は再生処理を停止し、ステップＳＰ２２に移って復号化処理手順を終了する。

【００８３】このようにＣＰＵ３０は、各素材に対応する記録映像データＤ４Ａ～Ｄ４Ｎを再生するために必要である暗号ＵＭＩＤデータＤ１２Ａ～Ｄ１２Ｎ及び暗号化データＤ１６Ａ～Ｄ１６Ｎ、Ｄ１７Ａ～Ｄ１７ＮをＩＥＥＥ１３９４インターフェイス３１を介して取得し、記録映像データＤ４Ａ～Ｄ４Ｎを順次再生する度に、その記録画像データＤ４に対応する暗号ＵＭＩＤデータＤ１２を復号化鍵Ｄ２０で復号化して得られたＵＭＩＤデータ１１に基づく素材特定暗号化鍵Ｄ１３で当該素材に対応する暗号化データＤ１６及びＤ１７を順次復号化することにより元のデータ並替パターンであるシャフリングテーブルデータＤ１４及びインターリーブテーブルデータＤ１５を復元することができる。

【００８４】その結果ＣＰＵ３０は、シャフリングテーブルデータＤ１４及びインターリーブテーブルデータＤ１５に対応するデータ並戻パターンであるデシャフリングテーブルデータＤ２２及びデインターリーブテーブルデータＤ２３を用いて１本のビデオカセット５の磁気テープ２０に記録された記録映像データＤ４Ａ～Ｄ４Ｎをそれぞれ素材毎に順次再生することができる。

【００８５】以上の構成において、ネットワーク対応型暗号化システム１におけるビデオカメラ２は、各素材が入力される度にその各素材をそれぞれ特定するためのＵＭＩＤデータＤ１１を生成し、各素材にそれぞれ対応する当該ＵＭＩＤデータＤ１１を暗号化鍵Ｄ１０の数学的条件に合わせる変換を行うことにより各素材毎に固有な素材特定暗号化鍵Ｄ１３を生成する。

【００８６】この素材特定暗号化鍵Ｄ１３は、素材毎に類推され難い固有な情報（ＵＭＩＤデータＤ１１に含まれるマテリアルナンバ）を暗号化鍵Ｄ１０の数学的条件に合わせる変換が行われているので、第三者にとっては暗号化鍵Ｄ１０のアルゴリズム、また素材毎に特定されたＵＭＩＤデータＤ１１に基づいて素材特定暗号化鍵Ｄ１３に変換する変換パターン、さらにはＵＭＩＤデータＤ１１に含まれる固有な情報（マテリアルナンバ）の全てが分からなければ到底解読し得ない情報である。

【００８７】そしてビデオカメラ２は、かかる素材特定暗号化鍵Ｄ１３で各素材毎に対応したそれぞれ異なるデータ並替パターン（シャフリングテーブルデータＤ１４及びインターリーブテーブルデータＤ１５）をそれぞれ暗号化することにより、各素材に対応した暗号化データＤ１６及びＤ１７を生成する。

【００８８】ここで、データ並替パターンは、磁気テープ２０に記録され記録される前の過程で素材を並び替えるものであり、ビデオテープレコーダ３が再生するにはそのデータ並替パターンが分からなければ元の素材に復元できないので、記録画像データＤ４を再生するために必要不可欠な情報である。

【００８９】従ってビデオカメラ２は、記録画像データＤ４そのものよりも一段と少ないデータ量であるデータ並替パターンを暗号化するだけで、あたかも記録画像データＤ４そのものを暗号化したものと同様の効果を得ることができる。

【００９０】これに加えてビデオカメラ２は、素材毎に生成したデータ並替パターンに対応する素材特定暗号化鍵Ｄ１３で暗号化しているので、仮に１つの暗号化データが解読された場合においても残り全ての暗号化データ１つ１つを再び解読させるようになされていることにより、結果として残り全ての暗号化データが直ちに解読されることを防止することができる。

【００９１】一方、ネットワーク対応型暗号化システム１における暗号化鍵Ｄ１０に対応する復号化鍵Ｄ２０を予め内部に記憶しているビデオテープレコーダ３は、各素材であるエレメンタルストリームＤ１が入力される度にその各素材をそれぞれ特定するために生成されたＵＭＩＤデータＤ１１と、当該ＵＭＩＤデータＤ１１に基づく各素材毎に固有な素材特定暗号化鍵Ｄ１３でデータ並替パターンをそれぞれ暗号化することにより生成された暗号化データＤ１６及びＤ１７とを暗号化装置から取得し、各素材にそれぞれ対応するＵＭＩＤデータＤ１１を暗号化鍵Ｄ１０の数学的条件に合わせる変換を行うことにより素材特定復号化鍵Ｄ２１を生成し、その素材特定復号化鍵Ｄ２１で暗号化データＤ１６及びＤ１７をそれぞれ復号化することにより、暗号化装置で暗号化される前の元のデータ並替パターンを復元することができる。

【００９２】以上の構成によれば、ネットワーク対応型暗号化システム１におけるビデオカメラ２では、各素材が入力される度にその各素材をそれぞれ特定するためのＵＭＩＤデータＤ１１を暗号化鍵Ｄ１０の数学的条件に合わせる変換を行うことにより得られた各素材毎に固有な素材特定暗号化鍵Ｄ１３で、データ並替パターン（シャフリングテーブルデータＤ１４及びインターリーブテーブルデータＤ１５）をそれぞれ暗号化するようにしたことにより、第三者にとっては暗号化鍵Ｄ１０のアルゴリズム、また素材毎に特定されたＵＭＩＤデータＤ１１

に基づいて素材特定暗号化鍵Ｄ１３に変換する変換パターン、さらにはＵＭＩＤデータＤ１１に含まれる固有な情報（マテリアルナンバ）の全てが分からなければ到底解読し得ない素材特定暗号化鍵Ｄ１３を生成することができ、かくして、第三者によって容易にデータ並替パターンが解読されることを防止することができる。

【００９３】なお、本実施の形態においては、インターネット４を経由して暗号ＵＭＩＤデータＤ１２、暗号化データＤ１６及びＤ１７をビデオカメラ２からビデオテープレコーダ３に送信する暗号化システムとしてのネットワーク対応型暗号化システム１に適用する場合について述べたが、本発明はこれに限らず、インターネット４に代えて、ディジタル衛星放送等の有線及び無線通信媒体を経由しても良く、また図１との対応部分に同一符号を付して示す図１２におけるパッケージメディア対応型暗号化システム５０のように、メモリカード５１を介して暗号ＵＭＩＤデータＤ１２、暗号化データＤ１６及びＤ１７をビデオカメラ２からビデオテープレコーダ３に受け渡すようにしても良い。

【００９４】この場合ネットワーク対応型暗号化システム１においては、取得手段としてのＣＰＵ３０（図１０）が暗号ＵＭＩＤデータＤ１２、暗号化データＤ１６及びＤ１７をＩＥＥＥ１３９４インターフェイス３１から取得するが、パッケージメディア対応型暗号化システム５０においては、取得手段としてのＣＰＵ３０がＩＥＥＥ１３９４インターフェイス３１に代わる読み出し手段としてのメモリカードインターフェイスを介して取得するようにしても良い。

【００９５】また上述の実施の形態においては、固有情報生成手段としてのＣＰＵ１０及びＵＭＩＤ生成部２１が固有情報としてのＵＭＩＤを生成し、当該ＵＭＩＤのうちＵＭＩＤデータＤ１１を抽出する場合について述べたが、本発明はこれに限らず、少なくともシリアルナンバ等の管理情報に乱数を乗じた固有情報を生成する固有情報生成手段であれば良い。このようにすれば、一段と少ないデータ量で素材である画像データを特定することができる。

【００９６】さらに上述の実施の形態においては、ＣＰＵ１０及び素材特定暗号化鍵生成部２３によって暗号化鍵生成手段を構成し、ＣＰＵ３０及び素材特定復号化鍵生成部４２によって復号化鍵生成手段を構成する場合について述べたが、本発明はこれに限らず、他の種々の回路構成によって暗号化鍵生成手段及び復号化鍵生成手段を構成するようにしても良い。

【００９７】さらに上述の実施の形態においては、暗号化手段としてのＣＰＵ１０及びテーブル暗号化部２５が暗号化対象としてのデータ並替パターンを暗号化することにより暗号化データＤ１６及びＤ１７を生成し、暗号復号化手段としてのＣＰＵ３０及びテーブル復号化部４３が当該暗号化データＤ１６及びＤ１７を復号化することにより元のデータ並替パターンを復元する場合について述べたが、本発明はこれに限らず、暗号化手段が記録ボタンが押下される度に入力した暗号化対象としての素材である画像データそのものを暗号化し、復号化手段素材が暗号化された当該素材である画像データを復号化するようにしても良い。

【００９８】この場合インターネット４を経由してビデオテープレコーダ３に送信する情報としては、暗号ＵＭＩＤデータＤ１１のみで良い。

【００９９】さらに上述の実施の形態においては、送信手段としてのＣＰＵ１０及びＩＥＥＥ１３９４インターフェイス１１が固有情報としてのＵＭＩＤデータＤ１１を暗号化することにより生成した暗号ＵＭＩＤデータＤ１２、暗号化データＤ１６及びＤ１７を送信し、受信手段としてのＣＰＵ３０及びＩＥＥＥ１３９４インターフェイス３１が当該暗号ＵＭＩＤデータＤ１２、暗号化データＤ１６及びＤ１７を受信する場合について述べたが、本発明はこれに限らず、少なくとも固有情報と暗号化データとを送信する送信手段及び受信手段であれば良い。

【０１００】さらに上述の実施の形態においては、非対象暗号化方式のＲＳＡに従った暗号化鍵Ｄ１０及び復号化鍵Ｄ２０を用いる場合について述べたが、本発明はこれに限らず、例えば対象暗号化方式のＤＥＳ(Data Encryption Standard)に従った暗号化鍵及び復号化鍵を用いる等、他の種々の暗号アルゴリズムに従った暗号化鍵及び復号化鍵を用いるようにしても良い。このようにすれば、インターネット対応型暗号化システム１を構築する状況に応じて、各種暗号アルゴリズムの特徴を効率よく選択することができる。

【０１０１】さらに上述の実施の形態においては、素材として画像データを適用する場合について述べたが、本発明はこれに限らず、例えば音声データ等、他の種々のデーOを素材として適用することができる。

【０１０２】さらに上述の実施の形態においては、暗号化装置としてのビデオカメラ２及び復号化装置としてのビデオテープレコーダ３を適用する場合について述べたが、本発明はこれに限らず、例えば画像データや音声データ等の素材を編集するための編集装置、ＣＤ(Compact Disk)プレーヤやパーソナルコンピュータ等、他の種々の暗号化装置及び復号化装置に幅広く適用することができる。

【０１０３】

【発明の効果】上述のように本発明によれば、各素材が入力される度に当該各素材をそれぞれ特定するための固有情報を生成し、各素材にそれぞれ対応する固有情報を所定の方式に従って変換して各素材毎に固有な暗号化鍵を生成し、その暗号化鍵で各素材又は各素材に対応した所定の情報をそれぞれ暗号化するようにしたことにより、類推し難い固有情報の全てが分からなければ第三者

にとっては到底解読し得ない固有な素材毎の暗号化鍵を生成することができ、かくして、第三者によって容易に暗号化対象が解読されることを防止することができる。

【０１０４】また各素材毎に対応した所定の情報として、各素材が入力される度にその各素材を所定データ量単位でそれぞれ並び替えるためのデータ並替パターンを暗号化するようにしたことにより、素材そのものを暗号化するよりも一段と少ないデータ量で暗号化することができる。

【０１０５】また上述のように本発明によれば、各素材が入力される度に当該各素材をそれぞれ特定するために生成された固有情報と、当該固有情報に基づく各素材毎に固有な暗号化鍵で各素材又は各素材に対応した所定の情報をそれぞれ暗号化して生成された暗号化データとを暗号化装置から取得し、各素材にそれぞれ対応する固有情報を所定の方式に従って変換して暗号化データをそれぞれ復号化するための復号化鍵を生成し、その復号化鍵で暗号化データをそれぞれ復号化して各素材又は各素材に対応した所定の情報を復元することにより、類推し難い固有情報と、当該固有情報に基づいて生成されているために第三者にとっては到底解読し得ない固有な素材毎の暗号化鍵とを取得して復号化鍵を生成することができ、かくして、確実かつ正確に各素材又は各素材に対応した所定の情報毎を復元することができる。

【０１０６】さらに上述のように本発明によれば、各素材が入力される度に当該各素材をそれぞれ特定するための固有情報を生成し、各素材にそれぞれ対応する固有情報を所定の方式に従って変換して各素材毎に固有な暗号化鍵を生成し、その暗号化鍵で各素材又は各素材に対応した所定の情報をそれぞれ暗号化して暗号化データを生成し、暗号化データと固有情報とを送信する暗号化装置と、当該暗号化データと固有情報とを受信し、各素材にそれぞれ対応する固有情報を所定の方式に従って変換して暗号化データをそれぞれ復号化するための復号化鍵を生成し、その復号化鍵で暗号化データをそれぞれ復号化して各素材又は各素材に対応した所定の情報を復元する暗号復号化装置とを構築するようにしたことにより、暗号化装置では、類推し難い固有情報の全てが分からなければ第三者にとっては到底解読し得ない固有な素材毎の暗号化鍵を生成することができるので、当該第三者によって容易に暗号化対象が解読されることを防止することができ、暗号復号化装置では、送信手段を介して類推し難い固有情報と、当該固有情報に基づいて生成されているために第三者にとっては到底解読し得ない固有な素材毎の暗号化鍵とを受信して復号化鍵を生成することができるので、確実かつ正確に各素材又は各素材に対応した所定の情報毎を復元することができる。

【０１０７】さらに上述のように本発明によれば、各素材が入力される度に当該各素材をそれぞれ特定するための固有情報を生成し、各素材にそれぞれ対応する固有情報を所定の方式に従って変換して各素材毎に固有な暗号化鍵を生成し、その暗号化鍵で各素材又は各素材に対応した所定の情報をそれぞれ暗号化して暗号化データを生成し、暗号化データと固有情報とを所定の記憶媒体に記憶する暗号化装置と、その暗号化データと固有情報とを当該記憶媒体から読み出し、各素材にそれぞれ対応する固有情報を所定の方式に従って変換して暗号化データをそれぞれ復号化するための復号化鍵を生成し、その復号化鍵で暗号化データをそれぞれ復号化して各素材又は各素材に対応した所定の情報を復元する暗号復号化装置とを構築するようにしたことにより、暗号化装置では、類推し難い固有情報の全てが分からなければ第三者にとっては到底解読し得ない固有な素材毎の暗号化鍵を生成することができるので、当該第三者によって容易に暗号化対象が解読されることを防止することができ、暗号復号化装置では、記憶手段から読み出した類推し難い固有情報と、当該固有情報に基づいて生成されているために第三者にとっては到底解読し得ない固有な素材毎の暗号化鍵とを受信して復号化鍵を生成することができるので、確実かつ正確に各素材又は各素材に対応した所定の情報毎を復元することができる。

【図面の簡単な説明】

【図１】本発明によるネットワーク対応型暗号化システムの構成を示す略線図である。

【図２】ディジタルビデオカメラレコーダの構成を示すブロック図である。

【図３】暗号化処理手順を示すフローチャートである。

【図４】ＵＭＩＤのデータ構造を示す略線図である。

【図５】データ並替パターン決定画面を示す略線図である。

【図６】シャフリング処理の説明に供する略線図である。

【図７】シャフリング処理の説明に供する略線図である。

【図８】リードソロモン符号生成の際の説明に供する略線図である。

【図９】素材毎に記録された記録画像データと、暗号ＵＭＩＤデータ及び暗号化データとの対応関係を示す略線図である。

【図１０】ディジタルビデオテープレコーダの構成を示すブロック図である。

【図１１】復号化処理手順を示すフローチャートである。

【図１２】他の実施の形態におけるパッケージメディア対応型暗号化システムの構成を示す略線図である。

【符号の説明】

１、５０……ネットワーク対応型暗号化システム、２……ビデオカメラ、３……ビデオテープレコーダ、４……インターネット、５……ビデオカセット、１０、３０……ＣＰＵ、１１、３１……ＩＥＥＥ１３９４インターフ

ェイス、１２、３２……メモリ、１３、３４……入力部、１４……表示部、１６……シャフリング部、１７、３７……ＥＣＣ部、１８……インターリーブ部、１９、３９……磁気ヘッド、２０……磁気テープ、２１……ＵＭＩＤ生成部、２２……ＵＭＩＤ暗号化部、２３……素材特定暗号化鍵生成部、２４……テーブル生成部、２５＊……テーブル暗号化部、２７……記録部、３３……ＨＤＤ、３６……デシャフリング部、３７……デインターリーブ部、４０……鍵生成部、４１……ＵＭＩＤ復号化部、４２……素材特定復号化鍵生成部、４３……テーブル復号化部、４５……再生部。

【図１】

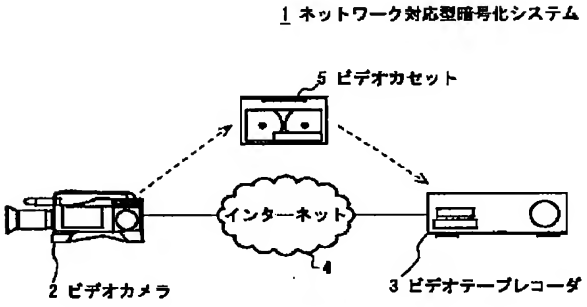


図１　ネットワーク対応型暗号化システムの構成

【図８】

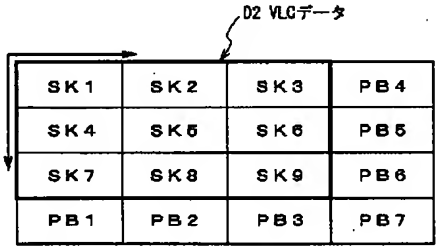


図８　リードソロモン符号の生成状態

【図２】

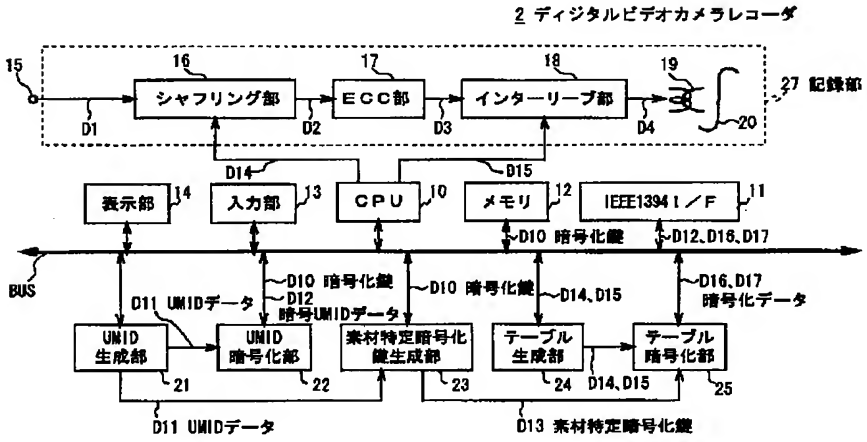


図２　ディジタルビデオカメラレコーダの構成

【図４】

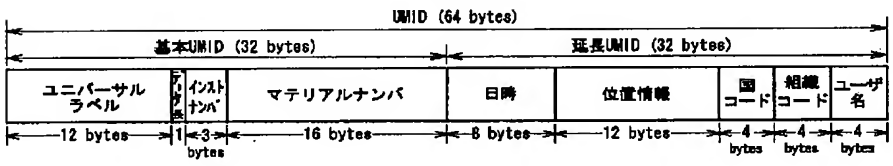


図４　ＵＭＩＤのデータ構造

【図３】

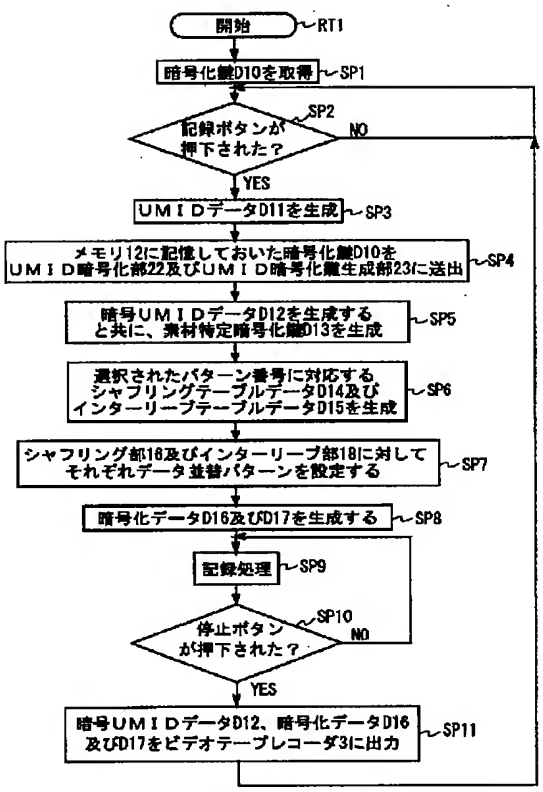


図３　暗号化処理手順

【図５】

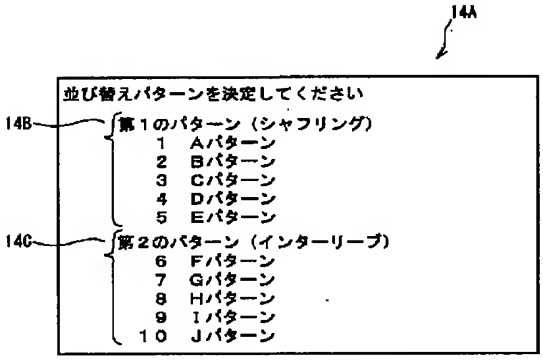


図５　データ並替パターン決定画面

【図７】

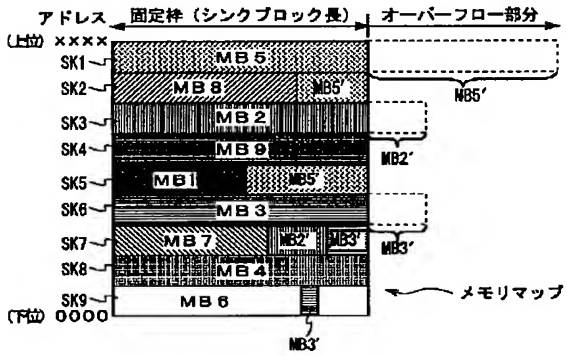


図７　シャフリング処理における内部メモリへの書き込み状況（２）

【図６】

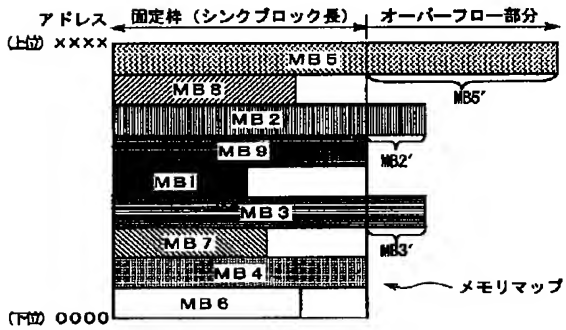


図６　シャフリング処理における内部メモリへの書き込み状況（１）

【図９】

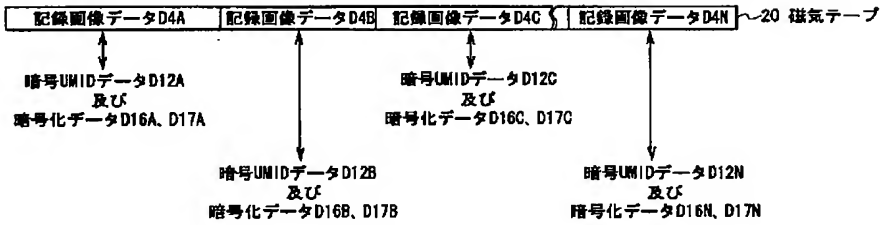


図９　素材毎に記録された記録画像データと、暗号UMIDデータ及び暗号化データとの対応関係

【図１０】

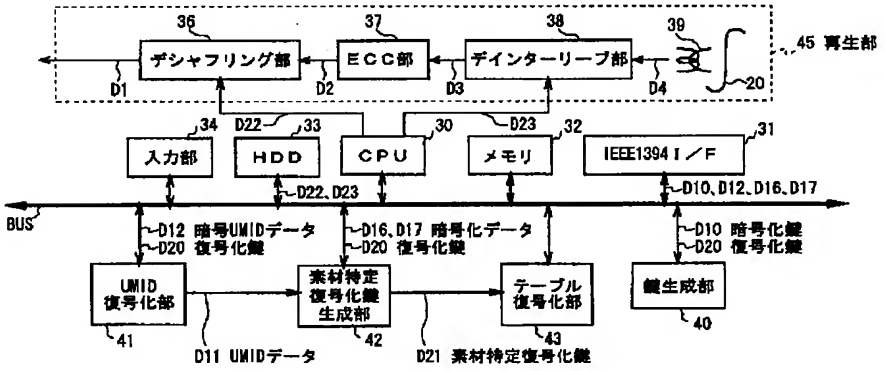


図１０　ディジタルビデオテープレコーダの構成

【図１２】

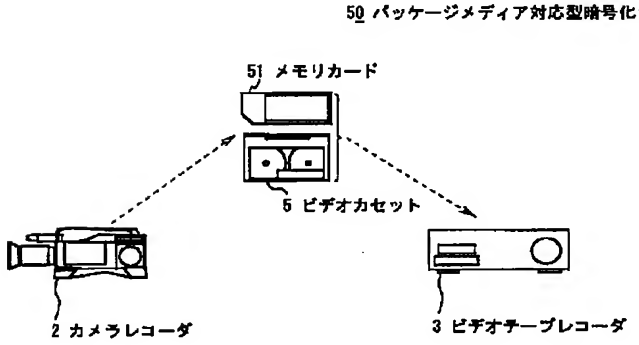


図１２　他の実施の形態におけるパッケージメディア対応型暗号化システムの構成

【図１１】

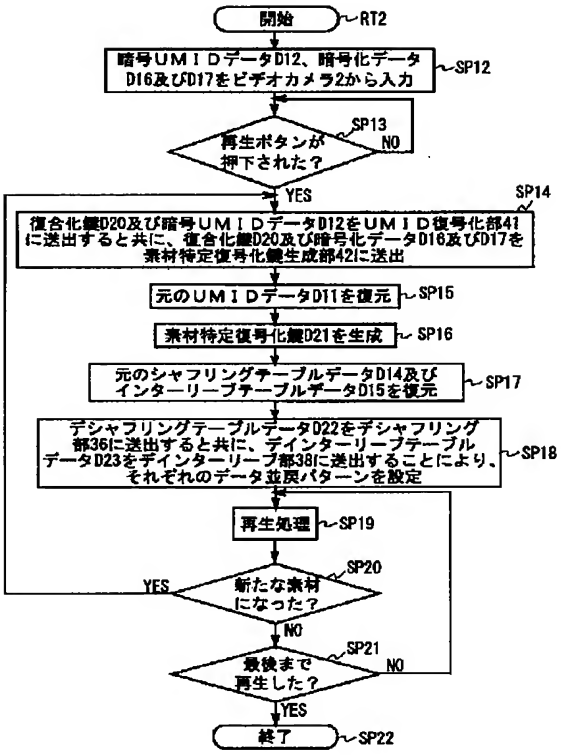


図１１　復号化処理手順